

ARTICLE APPEARED
ON PAGE 2A

WASHINGTON TIMES
16 April 1985

Hill panel seeks to pull plug on Soviet spies

By Ted Agres
THE WASHINGTON TIMES

The Senate Intelligence Committee is attempting to find out how to unplug the Soviet "vacuum cleaner" to protect U.S. scientific and technological secrets, the head of the panel says.

Sen. David Durenberger, R-Minn., chairman of the Senate Select Committee on Intelligence, told The Washington Times in an interview that one study will seek to evaluate security issues involving information transmission in the United States.

"We are sensitive to the fact that they [the Soviets] may have a greater capability [to eavesdrop] than we give them credit for in terms of how we communicate," Mr. Durenberger explained.

The Soviets, he said, use the "vacuum cleaner" approach to collect U.S. secrets.

Mr. Durenberger's comments follow closely a Reagan administration announcement that it was planning to equip hundreds of thousands of government offices with new, bug-proof "secure" telephones to counter electronic espionage.

Last month, the National Security Agency, which is responsible for, among other things, keeping U.S. government communications secure, announced that three U.S. firms had been chosen to build the new generation computerized scrambler telephones.

The three firms, RCA, AT&T and Motorola, reportedly will share a \$44 million grant to develop the new phones.

NSA said the new phones could be placed in up to half a million government and government contractor offices within five years. The scramblers, which will be about the size of a standard multi-

line office telephone, are expected to cost about \$2,000 each.

Government officials have said that U.S. secrets and sensitive information are being siphoned off by other governments, especially the Soviet Union. If an eavesdropper should intercept a conversation between two secure telephones, he will hear only a scrambled signal.

The situation with Soviet espionage has become so critical that last October President Reagan authorized the formation of a Cabinet-level group to attempt to counter it.

Mr. Reagan signed National Security Decision Directive 145, which established a Systems Security Steering Group to evaluate the problem and seek solutions. Members of the SSSG include the secretaries of State, Treasury and Defense, the attorney general, director of the Office of Management and Budget, and director of Central Intelligence.

An unclassified version of NSDD 145 released afterward stated that, "the compromise of [U.S.] information, especially to hostile intelligence services, does serious damage to the United States and its national security interests."

"A comprehensive and coordinated approach must be taken to protect the government's telecommunications and automated information systems against current and anticipated threats," the directive stated.

"This approach must include mechanisms for formulating policy, for overseeing systems security resources programs and for coordinating and executing technical activities."

The Cabinet-level steering group will oversee activities of a newly created, high-level Information Systems Security Committee, which is to focus on telephone and computer security as two top priorities.

Later today, Senate investigators will hold hearings on the government's ability to conduct background security investigations for personnel cleared to handle sensitive information.

The Senate Permanent Subcommittee on Investigations will look into the problems that have arisen. Sen. Sam Nunn, D-Ga., a member of the panel, was quoted as saying, "the government is already plainly incapable of adequately investigating and reinvestigating all persons seeking security clearances."

He added that the more than 4 million Americans who have security clearances are potential targets for the Soviet KGB.

The potential for electronic eavesdropping was highlighted recently when it was revealed that the Soviets had hidden bugs in about a dozen IBM typewriters in the U.S. Embassy in Moscow.

The tiny devices apparently detected the striking of individual keys and transmitted signals to antennas hidden in the building's walls, where the information was relayed to Soviet receivers.

A knowledgeable intelligence source in Washington told The Times that the incident highlights a horrible lack of

security at the embassy. But, the source added, the information that was compromised was not among the most sensitive that the embassy deals with.

High-level information is handled in special rooms designed to keep signals from leaking out, the source said. This technology of electronic containment is called "Tempest," and it involves placing copper shielding around typewriters, computer terminals or otherwise insulating the room.

Intelligence experts say that every communications device radiates weak electrical interference that can be picked up by sensitive electronic instruments called spectrum analyzers.

The interference patterns can be stripped away by computer to reveal the content of the message being handled, they say.

The NSA, which is based at Fort Meade, Md., about halfway between Baltimore and Washington, is trying to insulate its main operations building from electronic espionage.

Late last month, the agency told a House subcommittee it was seeking \$12.7 million to "Tempest-proof" its headquarters with an "electromagnetic envelope" to prevent spying.

In his interview with The Times, Mr. Durenberger also stated that the Senate Intelligence Committee will do a "long-term assessment of technology and, within that, a sense of technology security."

He said that some technology is inherently costlier in terms of security risks than other technology. He said that those factors haven't previously entered into the committee's long-range budget process.

"This obviously has some political judgment. To have a so-called security factor is important," he said.

The Minnesota senator also said that a similar study will be conducted regarding human intelligence, or "humint" as it is called.

"We're going to try to figure out why we are so weak in so many areas of humint," he said.

"We already know that we don't help the intelligence community think long-range in that regard; we don't educate and help them plan five years before there might be a problem, or 10 years before they are ever needed," he said.

STAT